ROTHERHAM METROPOLITAN BOROUGH COUNCIL
REPORT TO DEPUTY LEADER MEETING

1.	**Meeting:**	**Deputy Leader Meeting**
2.	**Date:**	**17th March 2014**
3.	**Title:**	**Baseline Personnel Security Standard for Public Service Network Use**
4.	**Directorate**	**Resources/Environment and Development Services**

5. Summary

To outline the new security checking arrangements required for users of the Public Services Network (PSN) to ensure compliance.

For the purpose of this report a "user of PSN services" is currently any RMBC computer user who consumes data which originates from PSN.
By the 2015 all RMBC computer users will fall in the category of 'PSN users'. (not including schools)

6. Recommendations

Deputy Leader meeting is asked to:

- **Agree a funding method for the required disclosure checks (both for retrospective and future checks)**
- **Confirm agreement with proposed approach i.e. focus on employees with less than three year service.**

7. Proposals and Details

7.1 Background

The Public Services Network Code of Connection (PSN CoCo) is a test of a council's information security and data protection maturity. PSN accreditation is administered by the National Technical Authority for Information Assurance and, ultimately, the Cabinet Office. The Council achieved connection to the Public Services Network towards the end of 2013 and were only the fourth council in the country to make the transition from the old Government Connect connection.

PSN provides us with:

- A faster and more secure network
- Access to a range of critical services such as Blue Badge, Revenues and Benefits, Registrars and Elections
- Secure data-sharing between all UK public sector organisations.
- Access to the 'G-Cloud'- this is a secure market place and hosting environment provided by Central Government. It enables any part of the UK public sector to procure hundreds of different cloud based services.

The Council has been approached by the Cabinet Office to act as an exemplar and reference site to assist other councils in achieving PSN compliance.

7.2 Employee checks

Having achieved connection to PSN we are now audited on an annual basis to ensure we are still compliant. Our next compliancy audit is due in September 2014. However, the Cabinet Office has recently tightened the rules around the use of PSN which now makes it harder to achieve compliance/accreditation. They have also adopted a 'zero tolerance' stance for any controls not met. This means that failure to comply with any control will result in disconnection from the PSN network and loss of the services mentioned above.

One of the tightened controls is the security check requirements for employees who will have access to the PSN network.

They have stated that we must:

"…ensure that any user, supplier or 3rd party involved in the consumption or provision of PSN Services receives appropriate security vetting. The vetting standards shall be based on the Baseline Personnel Security Standard (BPSS) or comparable."

The BPSS requires all employees to have undergone:

- An identity check
- A check of Nationality and Immigration status
- Clarification of employment history (for the past three years)
- Verification of Criminal Record (unspent convictions only i.e. Basic Disclosure check)

The Council achieved PSN compliance in 2013 despite having yet to fully adopt BPSS checking as our current processes where considered robust

enough at that time . However, with the recent tightening of compliance criteria for the 2014 audit we must improve the rigour with which we security check employees and ensure we have adhered to all the requirements outlined in the BPSS if we are to be re-accredited to use the PSN.

Due to the large numbers of employees this will involve and the expense and time required to undertake BPSS level of checking, the Cabinet Office have allowed councils to undertake the process on a staged basis.

Stage One – All users of PSN services or data by 2013 (400 employees for RMBC). Although satisfactory for 2013 compliance these employees will now need to be further security checked to ensure we have covered all elements of the BPSS.
Stage Two – All users of PSN email by 2014 (a further 200 employees making 600 RMBC employees in total)
Stage Three – All users of PSN connected network by 2015 (added to those from the previous two stages this makes a total of 4,500 RMBC computer using employees)

Although the staged approach will help councils to achieve the standard required the Cabinet Office is currently being challenged on this requirement by both the Regional Warning Alert Reporting Partnership (i.e. IT security and Information Governance) plus the Regional Employers Group. The challenge concerns the additional costs and resources required to meet the requirement. At present there is no indication that the Cabinet Office will soften their stance on this issue.

7.3 Current position
As mentioned above, for Stage One, we have identified that this will involve 400 current employees, 200 for Stage Two and for Stage Three the remainder of the computer using workforce making a grand total of 4,500 employees who need security checking to BPSS level.

This figure does not include schools because at present time the Schools network is suitably segregated for us not to include them. This situation may change in the future. We have also not included some frontline employees as they currently have no direct access to PSN. However, the introduction of hand held devices and other technology in the future may require this employee group to be included in the full checking process.

The Council already routinely checks new starters to a level which complies with some elements of BPSS.

- Identity checks – we currently identity check all new starters to the Council through verification of specific documents.

- Check of Nationality and Immigration Status – again these checks are undertaken as part of the recruitment process for all new starters.

  For the above two points it should be noted that this only became a legal requirement following the introduction of the Immigration, Asylum and Nationality Act 2006. Therefore any employee who started working for

the Council prior to this legislation coming into force will not have been subject to this checking process.

- Clarification of employment history – reference checks are undertaken with previous employers as part of the recruitment process. However this does not necessarily always cover the BPSS specified three year period.

- Verification of criminal record – these are only carried out for specific posts that involve caring for, supervising or being in sole charge of children or adults. These checks are more detailed and therefore more costly as they are undertaken at the Enhanced level. We currently do not undertake any Basic Disclosure Checks.

7.4 Proposed action

Other councils have apparently achieved accreditation by demonstrating that their ID checking processes are robust, even if they do not go as far as a full BPSS check for all employees. Given the recent zero tolerance statement by the Cabinet Office we consider this approach to be 'too risky'. However, we do believe that a 'risk based' approach to this PSN control may be acceptable if we can clearly justify the reasons.

Our recommended approach does meet the BPSS compliance (unlike the other councils mentioned above) but argues that the majority of the Council's workforce have been in our employ for over three years (the employment history check requirement) and are therefore deemed to be 'known and trusted' employees. At the same time we will commit to checking all new employees and those who have been with the Council for less than three years to the BPSS level within the recommended timescales.

Therefore, in order to be able to address the timescales outlined by the Cabinet Office and also to keep the resource requirements (both financial and physical) to a minimum we recommend the following:

- Given the BPSS asks for employment history checks for the last three years, for employees with three years or more continuous service with the Council – due to the amount of time the employee has been known to the Council it is felt that this level of checking is not appropriate and therefore no further checking will be required.

- For employees with less than three years employment with the Council – identity checks and Nationality and Immigration Status will have been undertaken at the recruitment stage. Personal files will be checked to ensure the three year employment history clarification requirement. If the references on file cover the outstanding period after RMBC employment is taken in account then no further action will be required. If the references + RMBC employment doesn't cover the three year period, we shall attempt to contact all previous employers until the time period has been met.

- Verification of Criminal Records (Basic Disclosure) – to be undertaken for all current employees with less than three years continuous service

With effect from the 1st April 2014 our recruitment processes will be amended to ensure all new employees to the Council have the relevant level of checks required for PSN compliance. Working with ICT, HR will update the HR and Payroll system to indicate which posts require the BPSS level of checking to ensure managers are clear which posts are affected. All relevant recruitment documentation (e.g. job profiles, guidance notes etc.) and training materials will also be updated to reflect the new requirements.

Subject to confirmation it is proposed the cost of this check will be charged to the recruiting manager.

8. Finance

Although this new level of security checking will require a good deal of additional officer time the most direct cost implication will be for the Basic Disclosure check. The cost for this is currently £32.50 per check (£25 for the check plus £7.50 admin costs).

If we implement the recommended approach out of the 4,500 employees who will require this level of checking there are currently only around 270 eligible employees with less than three years' service who will require a criminal records check at the Basic Disclosure level. The quantity is quite low as many social care employees have already been checked at the enhanced level. The cost for this element will be approximately £8,700. Currently there is no central fund to cover these costs therefore it is envisaged that it will have to be financed from existing local budgets, for which understandably no provision has been made.

If our recommended approach is not acceptable the costs will be significantly higher. As a quick rough estimate, taking into account social care employees will have already been checked at the enhanced level, there will still be in the region of 3,000 employees requiring the basic check. This will push the cost to around £100,000.

Going forward for new starters, based on the new starter figures for 2013/14 costs for this element would equate to approximately:

- Resources - £910
- NAS - £2,080
- EDS - £812
- CYPS - £845

9. Risks and Uncertainties

Failure to comply with this requirement could eventually result in disconnection from the PSN network and loss of the services outlined in point 7.1. As we are recommending instigating the three years' service cut off point there is a risk that auditors will consider we have not fully met the control.

There may also be employee relations issues to deal with if the Basic Disclosure checks reveal criminal convictions which have:

- Taken place whilst the individual has been in our employ
- Not been declared at the recruitment stage

Although a criminal conviction does not necessarily mean there is an issue, in some instances it might be considered to conflict with the job the employee is currently undertaking.

10. Policy and Performance Agenda
As this is a whole workforce issue it underpins all corporate priorities.

11. Background Papers and Consultation
Baseline Personnel Security Standard

Contact Name:
HR elements - Paul Cosgrove (HR Business Partner) paul.cosgrove@rotherham.gov.uk 01709 334160 and Debby Lamb (Senior HR Officer) debby.lamb@rotherham.gov.uk 01709 823701
ICT elements –Richard Copley (Corporate ICT Manager) richard.copley@rotherham.gov.uk 01709 254525 and Abi Dakin (ICT Compliance and Improvement Specialist) abi.dakin@rotherham.gov.uk 01709 823245